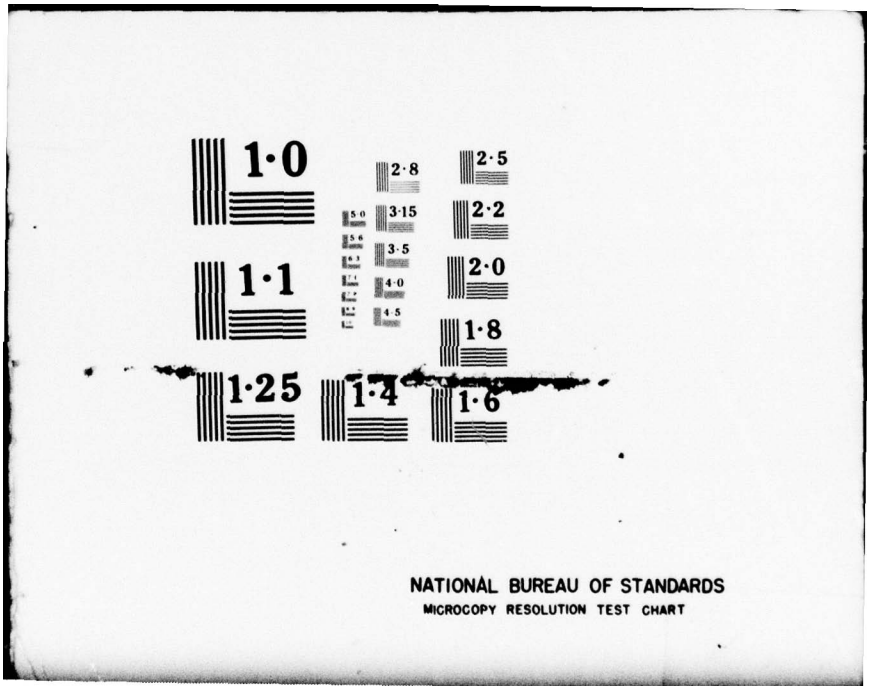
AD-A048 454 VIRGINIA POLYTECHNIC INST AND STATE UNIV BLACKSBURG F/G 17/2
QUADRATIC MULTIPLEXING--A NEW METHOD FOR SECURE COMMUNICATION.(U)
DEC 77 M J HINICH N00014-75-C-0494
UNCLASSIFIED TR-11 NL

1 OF 1
AD A048454

END
DATE FILMED
2-78
DDC


1·0
1·1
1·25
1·4
1·6
1·8
2·0
2·2
2·5
2·8
3·15
3·5
4·0
4·5
5·0
5·6
NATIONAL BUREAU OF STANDARDS
MICROCOPY RESOLUTION TEST CHART

QUADRATIC MULTIPLEXING--A NEW METHOD FOR SECURE COMMUNICATION

Melvin J. Hinich
Virginia Polytechnic Institute and State University
Blacksburg, Virginia

December 1977

Quadratic Multiplexing--A New Method for Secure Communication

Melvin J. Hinich
Virginia Polytechnic Institute and State University

December, 1977

Abstract

A secure digital multiplexing technique is presented which uses a pseudo-random process with a fundamental cycle length N. The method can handle D < N signal sequences of length M < N. The SNR's of the de-multiplexed signals is N/4DM for large N, even if the additive noise power is large. The de-multiplexer must compute the discrete Fourier transform of the pseudo-random sequence that is used to encode the signals. Information is carried in the phase differences between the frequency components of the multiplexed signal. De-multiplexing requires at least $DMN\log_2 N$ arithmetic calculations.

This work was supported by the Office of Naval Research under contract.

Quadratic Multiplexing--A New Method for Secure Communication

Melvin J. Hinich
Virginia Polytechnic Institute and State University

Introduction

This paper presents an information coding technique that increases the channel capacity of a communication link. This technique can be used with any reliable system for transmitting information from origin to destination. For a computer to computer transmission link, for example, a number of messages are combined into a signal which is transmitted by standard high frequency methods to a receiver which demodulates the signal into a replica of the original multiplexed signal. This signal is then unscrambled to yield the individual messages.

The increase in channel capacity results from information which is carried in the phase differences between frequency components of the broadband multiplexed signal, and thus the technique is inherently nonlinear.

Information is encoded using a cyclic pseudo-random process. The receiver must generate the same pseudo-random process that is used for encoding, making the technique secure from unauthorized interception. I will now discuss the pseudo-random process before going into details about signal processing.

1. A Discrete Pseudo-random Process

I will limit my exposition to discrete time processes and digital signal processing. The analogies with a continuous time system are straightforward.

Let $\{x(t_n)\}$ denote a discrete pseudo-random white noise process. The time index $t_n = nf_s^{-1}$, where n is an integer and f_s is the sampling frequency. Algorithms for generating sequences which appear to be random and uncorrelated are well known by now (for an example see Kronmal [1]). These algorithms produce sequences of numbers which satisfy the statistical properties of a stationary white noise process. One of the most widely used algorithms, the congruential generator, produces sequences that obey a uniform density on the (0,1) interval, although it has a fundamental period which is determined by the bit length of the computer registers, and the "seed" value used in the algorithm.

It will simplify the Fourier transform mathematics if $\{x(t_n)\}$ is periodic. Let N denote the fundamental cycle length, and thus $x(t_n) = x(t_{n+N})$ for all n. This cycle can be set by suitable choice of bit length, or by re-initializing the generator at n = N using the same seed value.

From here on, the $x(t_n)$ values will be treated as if they were realizations from a finite variance stationary white noise process, where for simplicity the expected value $Ex(t_n) = 0$ for all n.[1] That is, for all n $Ex(t_n + \tau)x(t_n) = 0$ for $\tau \neq 0$ (τ an integer multiple of f_s^{-1}) and $Ex^2(t_n) = \sigma_x^2$.

Define the discrete Fourier transform

$$X(f) = \sum_{n=0}^{N-1} x(t_n)\exp(-i2\pi f t_n) \quad . \tag{1}$$

The principal domain of X(f) is the band $0 \leq f < f_s$. Then it follows that for each n = 0,1,...,N-1

$$x(t_n) = \frac{1}{N} \sum_{k=0}^{N-1} X(f_k)\exp(i2\pi f_k t_n), \qquad (2)$$

where $f_k = (k/N)f_s$ are equally spaced discrete frequencies. Moreover $X(f_k) = X^*(f_{N-k})$ where the star denotes complex conjugate, and $X(f_{-k}) = X^*(f_k)$. Since $Ex(t_n) = 0$, $EX(f_k) = 0$.

The following three properties can easily be derived from the assumption that $\{x(t_n)\}$ is white. For each $k = 0,1,\ldots,N-1$

1) $\mathrm{Re}X(f_k)$ and $\mathrm{Im}X(f_k)$ are uncorrelated,

2) The variance of $X(f_k)$ is $E|X(f_k)|^2 = N\sigma_x^2$,

3) $X(f_k)$ and $X(f_\ell)$ are uncorrelated for $k \neq \ell$.

In addition, from the central limit theorem

4) $\{X(f_k):k = 0,\ldots,N-1\}$ have a complex Gaussian joint distribution in the limit as $N \to \infty$. For a discussion of the complex Gaussian distribution, see Brillinger [2].

2. Multiplexing The Signals

Suppose that D digitized signals of duration Mf_s^{-1} are to be multiplexed and transmitted. In order to simplify notation, let the time unit be the sampling interval f_s^{-1}, and supress the unit by setting $t_n = n$ for each n. Denote the D as follows: $\{a_1(0),\ldots, a_1(M-1)\},\ldots, \{a_D(0),\ldots,a_D(M-1)\}$. Assuming that D and M<N, each a_d signal is convolved with the lagged product sequence $\{\sigma_x^{-2}x(n)x(n-d)\}$. These convolutions are summed to form the quadratic multiplexed signal (Figure 1).

$$y(n) = \sum_{d=1}^{D} \sum_{m=0}^{M-1} a_d(m)\sigma_x^{-2}x(n-m)x(n-m-d). \qquad (4)$$

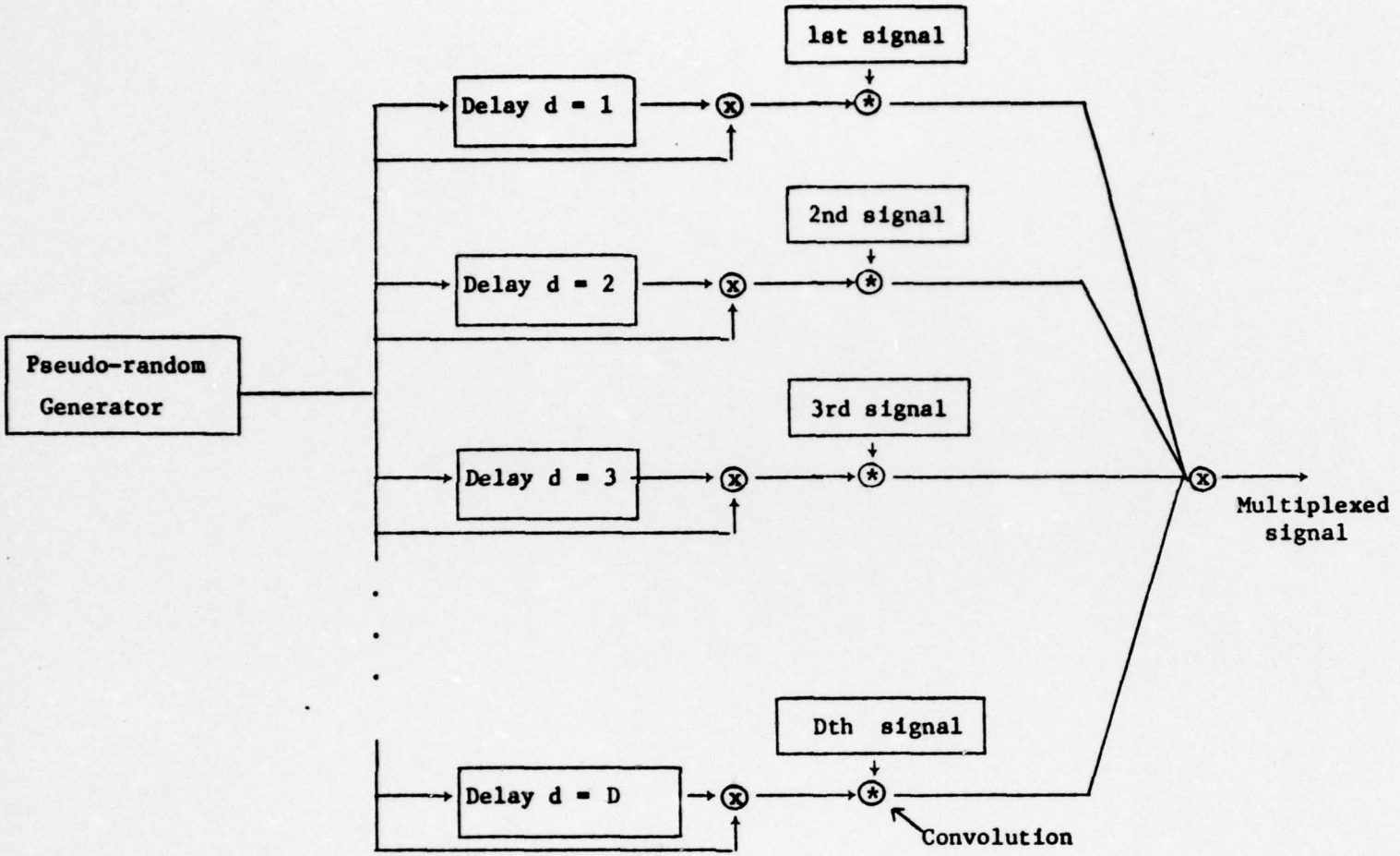


Figure 1. Quadratic Multiplexing

The signal {y(n)} is used to modulate a high frequency carrier. This modulated signal is then transmitted to receivers which have the same pseudo-random generator that is used to multiplex the signals.

Taking the Fourier transform of (4), we have

$$Y(f_k) = \sum_{d=1}^{D} A_d(f_k) N^{-1} \sum_{\ell=0}^{N-1} \sigma_x^{-2} X(f_{k-\ell}) \exp(-i2\pi f_\ell d), \tag{5}$$

where $f_k = \frac{k}{N}$ for k = 0, 1,..., N-1; and

$$A_d(f_k) = \sum_{m=0}^{M-1} a_d(m) \exp(-i2\pi f_k m) \tag{6}$$

are the Fourier transforms of the signals. If prior to digitizing all the signals were bandlimited at f_o, there is no aliasing if $f_s = 2f_o$ and the quadratic multiplexed signal will then have the same bandwidth as all the original signals.

For certain applications, such as speech transmission, it will be better to set M = N and use a much higher sampling rate than f_o, i.e. $f_s >> f_o$. At the receiver end, the de-multiplexed signals must be smoothed by a low pass filter of bandwidth f_o in order to have a high output SNR.

In order to facilitate the statistical analysis of the de-multiplexing technique, conceive of the signals as realizations from <u>independent</u> (zero mean) white Gaussian noise processes with equal variances. Let σ_a^2 denote the signal variance (power).

3. <u>De-multiplexing the Received Signal</u>

Suppose that the receiver digitizes the high frequency version of the multiplexed signal, yielding a time compressed y signal plus noise

denoted by $p(n) = y(n) + \varepsilon(n)$. Once again the time unit is supressed, but this unit is much smaller than the original sampling interval f_s^{-1} when the signal is time compressed.

In the frequency domain, $P(f_k) = Y(f_k) + e(f_k)$, where $\{e(f_k)\}$ is the Fourier transform of the noise. Even when N is large, the $P(f_k)$ values can be computed in a short time by using an IC module programmed with the FFT algorithm.

The receiver must have either the pseudo-random sequence $\{x(n)\}$, or its Fourier transform. Suppose that the receiver generates the unsynchronized sequence $\{x(n + \tau)\}$, where τ is an unknown shift. It will now be shown that the signals, delayed by τ units, can be extracted with a high SNR ratio when $N/DM>>1$.

Denote the Fourier transform of $\{x(n + \tau)\}$ by $X_\tau(f_k)$. Clearly $X_\tau(f) = X(f) \exp i2\pi f\tau$. Next define the weight function for each d and k,

$$W_d(k)=(\sigma_x N)^{-2} \sum_{j=0}^{N-1} X_\tau(f_j)X_\tau(f_{k-j})\exp(-i2\pi f_j d). \tag{7}$$

As is shown in Theorem 2 (Appendix), for each $m = 0,\ldots, M - 1$

$$s_d(m) = N^{-1} \sum_{k=0}^{N-1} W_d(k)P^*(f_k)\exp(-i2\pi f_k m) \tag{8}$$

$$= a_d(m-\tau) + \varepsilon_k, \tag{9}$$

where the ε_k are approximately uncorrelated Gaussian $N(0,4N^{-1}(DM\sigma_a^2+\sigma_\varepsilon^2))$. In other words, the double Fourier transform of the array $\{N^{-3}\sigma_x^{-2}X(f_j)X(f_{k-j})P^*(f_k)\}$ extracts the D signals with an output SNR of $N/4DM$ when $\sigma_\varepsilon^2<<N$. The NxN array is transformed using two successive

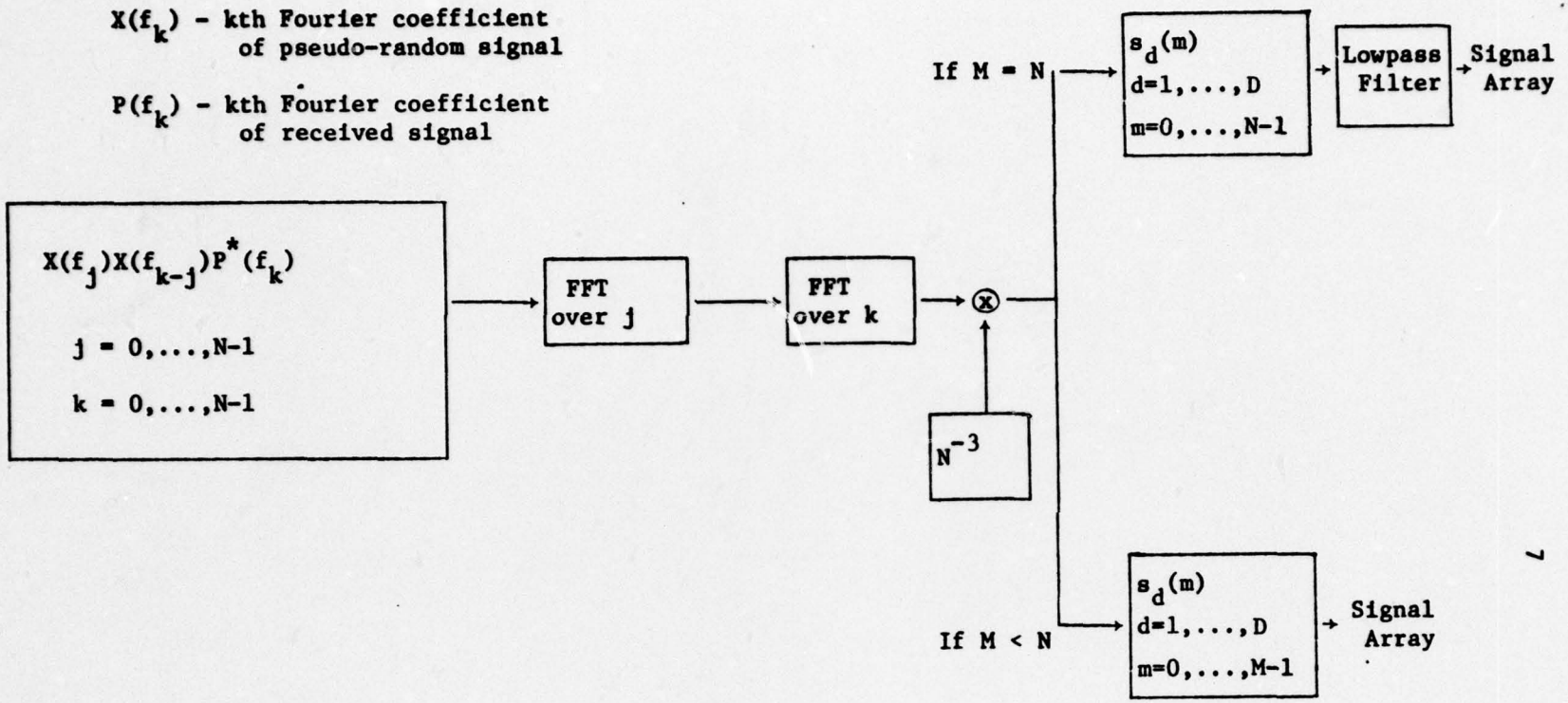


Figure 2. De-multiplexing

FFT's to yield an DxN array whose dth row is $a_d(m)$. When M<N, the last N-M columns are discarded. The first row (d=0) is $2N^{-1} \sum_{d=1}^{D} a_d(m-\tau)$.

The signals, however, are shifted by τ units. If the receiver can store the N complex numbers $\{X(f_k)\}$, there is no synchronization problem since expression (9) holds with $\tau = 0$. The signals are extracted with no delay if the receiver can store or compute $\{X(f_k)\}$. Note that the transforms in (7) and (8) can be efficiently computed using the FFT algorithm.

For applications where M = N and $f_s >> f_o$, then the output of the Fourier transform in (8) must be shifted back to the $(0, f_s/2)$ band and then smoothed by a low pass filter in order to increase the output SNR. The SNR will be $f_s/f_o D$ if the filter bandwidth is f_o.

4. Comparison with Time Division Multiplexing

The lagged product sequence $\{\sigma_x^{-2} x(n)x(n-d)\}$ can be thought of as an ensemble of sinusoidal carriers with frequencies $0<f<f_s$, unit amplitudes and random phases. The SNR for each signal is $\sigma_a^2/\sigma_\varepsilon^2$.

Using no security processing, suppose that the signals were time division multiplexed using a unit amplitude carrier. In order to achieve the output SNR of N/4DM, each signal would have to be repeated $\sigma_\varepsilon^{-2} N/4DM$ times. Consequently, at most $4D\sigma_\varepsilon^{-2}$ messages of length M could be multiplexed using a N long sequence, and thus the quadratic method handles more signals when $\sigma_\varepsilon^2 < 4$.

In any event, the quadratic method is secure. This security is achieved at the cost of computing ND FFT's during de-multiplexing. These FFT's can be performed by the main frame CPU for computer to computer communication.

Consider the following example. Let $\sigma_a^2 = 1$, $\sigma_\epsilon^2 = 10^3$, $M = 10^2$, and $D = 10^3$. The SNR for each signal is -30db. If $N = 5 \times 10^6$, then the output SNR of each of the 10^3 de-multiplexed signals is 11db ($N/4DM = 12\frac{1}{2}$ and $\sigma_\epsilon^2 << N$).

Rather than computing the DM array $\{s_d(m)\}$ by using DN FFT's, the double Fourier transform of $X(f_j)X(f_{k-j})P^*(f_k)$ can be computed for $d = 1,\ldots,D$ and $m = 0,\ldots,M-1$ by $DMN\log_2 N$ arithmetic steps using the idea behind the radix 2 FFT algorithm. The computations can be organized in a sequential manner so that the entire NxN array of the triple product does not have to be stored.

As a final note, another signal can be transmitted with no interference with the D signals by adding $\sum_{m=0}^{M-1} a_0(n)x(n-m)$ to $y(n)$. This linear component is uncorrelated with $y(n)$. Thus the $a_0(n)$ signal can be extracted by taking the Fourier transform of the sample cross spectrum between $\{x(n)\}$ and $\{p(n)\}$. The SNR is the same as that for the other signals.

Appendix

Theorem 1. The spectrum $S_y(f)$ of $\{y(n)\}$ is $\sum_{d=1}^{D} |A_d(f)|^2$. The spectrum of $\{p(n)\}$ is $S_y(f) + \sigma_\varepsilon^2$.

Proof: For each f, there exists a sequence k(N) such that $f_{k(N)} = \frac{k(N)}{N} \to f$ as $N\to\infty$. As is shown in [2], $S_y(f) = \lim_{N\to\infty} N^{-1}|Y(f_{k(N)})|^2$. In order to derive this limit, note that $EN^{-1}|X(f_k)|^2 = \sigma_x^2$ and thus $S_x(f) = \sigma_x^2$. Moreover by properties 3 and 4 (Introduction), $EX(f_j)X(f_k)X(f_\ell) = 0$. Applying these results to (5),

$$EN^{-1}|Y(f_k)|^2 = \sum_{r=1}^{D}\sum_{s=1}^{D} A_r(f_k)A_s^*(f_k)N^{-1}\sum_{j=0}^{N-1}\sum_{\ell=0}^{N-1} \exp i2\pi(f_\ell s - f_j r)\sigma_x^{-4}EN^{-2}X(f_{k-j})X(f_j)X^*(f_{k-\ell})X^*(f_\ell). \tag{A1}$$

For large N, it follows from properties 2, 3 and 4 that

$$\begin{aligned} EN^{-2}X(f_{k-j})X(f_j)X^*(f_{k-\ell})X^*(f_\ell) &= \sigma_x^4 \quad \text{if } j = \ell \neq k/2 \text{ or } j+\ell = k \\ &= 3\sigma_x^4 \quad \text{if } j = \ell = k/2 \\ &= 0 \quad \text{otherwise.} \end{aligned} \tag{A2}$$

Consequently, most of the cross terms in the second double sum are zero. Applying (A2) to (A1), $N^{-1}|Y(f_{k(N)})|^2 \to \sum_{d=1}^{D} |A_d(f)|^2$ as $N\to\infty$ since $\sum_{j=0}^{N-1} \exp i2\pi f_j(s-r) = 0$ if $r \neq s$, and $\lim_{N\to\infty} N^{-1}\sum_{j=0}^{k(N)} \exp i2\pi f_j(r+s) = 0$. When the signals are realizations from independent Gaussian white noise processes, $|A_d(f)|^2 \simeq M\sigma_a^2$. The spectrum of $\{p(n)\}$ is $S_y(f) + \sigma_\varepsilon^2$ since the errors are independent of the x's.

Theorem 2. Expression (9) holds. The error variance is approximately $4N^{-1}(DM\sigma_a^2 + \sigma_\varepsilon^2)$ for large N. Thus the output SNR is N/4DM.

Proof: First consider the case $\tau = 0$. From (5) and (A2),

$$\sigma_x^{-2}N^{-1}EX(f_j)X(f_{k-j})P^*(f_k) = \sum_{d=1}^{D} A_d^*(f_k)(\text{expi}2\pi f_j d + \text{expi}2\pi f_{k-j} d)$$

$$= \sum_{d=1}^{D} A_d^*(f_k)(\text{expi}2\pi f_j d + \text{expi}2\pi f_k d \exp(-i2\pi f_j d) \tag{A3}$$

if $j \neq k/2$. When $j = k/2$, the expected value is $3\sum_{d=1}^{D} A_d(f_k)\text{expi}2\pi f_{k/2} d$. Since $\sum_{j=0}^{N-1} \exp(-i2\pi f_{2j} d) = 0$ for each $d = 1,\ldots, N-1$, it follows from (7) and (A3) that for $\tau = 0$ and $d>0$,

$$EW_d(k)P^*(f_k) = N^{-2} \sum_{j=0}^{N-1} X(f_j)X(f_{k-j})P^*(f_k)\exp(-i2\pi f_j d)$$

$$= A_d^*(f_k) + O(DM/N) \tag{A4}$$

since $N^{-1}\sum_{d=1}^{D} A_d(f_k)\text{expi}2\pi f_{k/2} d$ is of the order O(DM/N).

Transforming (A4) into the time domain as shown in (8),

$$Es_d(m) = a_d(m) \qquad m = 0,\ldots,M-1 \tag{A5}$$

for large N. When $d = 0$, $Es_0(m) = 2N^{-1}\sum_{d=1}^{D} a_d(m)$.

When $\tau \neq 0$, the right hand side of (A4) is multiplied by $\text{expi}2\pi f_j \tau \ \text{expi}2\pi f_{k-j}\tau = \text{expi}2\pi f_k \tau$. Thus $Es_d(m) = a_d(m-\tau)$ plus an error whose distribution will now be derived using the stochastic assumptions for the signals.

The next step is to derive the asymptotic distribution of the errors $s_d - Es_d$. The term $B(j,k) = N^{-1}X(f_j)X(f_{k-j})P^*(f_k)$ is the sample cross bispectrum at f_k between $\{x(n)\}$ and the received signal. As is shown by Rosenblatt and Van Ness [3], the variance of $B(j,k)$ is $NS_x(f_j)S_x(f_{k-j})S_p(f_k)$. By Theorem 1, $S_p(f) = DM\sigma_a^3 + \sigma_\varepsilon^3$. Thus $\text{Var } B(j,k) = N\sigma_x^4(DM\sigma_a^2 + \sigma_\varepsilon^2)$.

For large N the $B(j,k)$ variates are uncorrelated in the triangular region $\{j = 0,\ldots,[k/2];\ k = 0,\ldots,N-1\}$. This triangle is called the principal domain of $B(j,k)$. The following symmetries relate the $B(j,k)$'s outside this domain to those in the domain:
$B(k/2 + \ell,\ k/2 - \ell) = B(k/2 - \ell,\ k/2 + \ell)$ for k even,
$B((k-1)/2 + \ell,\ (k+1)/2 - \ell) = B((k+1)/2 - \ell,\ (k-1)/2 + \ell)$ for k odd, and
$B^*(N-j,N-k) = B(j,k)$. Thus there are approximately $N^2/4$ degrees of freedom for the $B(j,k)$'s in the square $\{j = 0,\ldots,N-1;\ k = 0,\ldots,N-1\}$.

Expression (8) can be rewritten as follows:
$s_d(m) = (N\sigma_x^2)^{-2} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} B(j,k)\exp[-i2\pi(f_j d + f_k m)]$. By the central limit theorem, the variance of $s_d(m)$ is $4\sigma_x^{-4}N^{-2}\text{Var}B(j,k) = 4N^{-1}(DM\sigma_a^2 + \sigma_\varepsilon^2)$. The factor 4 results from the symmetries of the $B(j,k)$ in the double sum. Moreover, the $s_d(m)$ are uncorrelated for large N by the orthogonality inherent in Fourier transforms (property 3).

References

[1] R. Kronmal, "Evaluation of a pseudorandom normal number generator," J. Assoc. Comp. Mach. 11, 357-363, 1964.

[2] D. Brillinger, Ch. 4 Time Series, Data Analysis and Theory, N.Y.: Holt, Rinehart and Winston, 1975.

[3] M. Rosenblatt and J. W. Van Ness, "Estimation of the bispectrum, Ann. Math. Statist. 36 (4), 1120-1136, 1965.

Footnote

1. Simple whiteness is not sufficient to obtain the asymptotic results used in this paper. Assume, in addition, that $Ex(n_1)x(n_2)x(n_3) = 0$; $Ex^2(n_1)x^2(n_2) = \sigma_x^4$ if $n_1 \neq n_2$; and $Ex(n_1)x(n_2)x(n_3)x(n_4) = 0$ if $n_1 \neq n_2 \neq n_3 \neq n_4$. These conditions hold if the process is Gaussian.

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER (14) TR-11 Technical Report No. 11	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) (6) Quadratic Multiplexing--A New Method for Secure Communication		5. TYPE OF REPORT & PERIOD COVERED (9) Technical Report,
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) (10) Melvin J. Hinich		8. CONTRACT OR GRANT NUMBER(s) (15) N00014-75-C-0494
9. PERFORMING ORGANIZATION NAME AND ADDRESS Virginia Polytechnic Institute and State University		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS NR-042-315
11. CONTROLLING OFFICE NAME AND ADDRESS Office of Naval Research Code 436 Statistics and Probability Program Arlington, VA 22217		12. REPORT DATE (11) December 1977 (12) 16 p.
		13. NUMBER OF PAGES Twelve
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Reproduction in Whole or part is permitted for any purpose of the United States Government. Distribution is unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Multiplexing, Secure Communication, Discrete Fourier Transform, Cross Bispectrum

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

407206